AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising:

concatenating data from a plurality of fields of a requested web page into a string;

encrypting the string;

serving to a user node, the web page and a form corresponding to the requested web page that includes each blank field in the plurality of fields and the encrypted string; and

enabling at least the encrypted string to be locally decrypted to allow interacting with the decrypted string at the user node.

2. (Original) The method of Claim 1 further comprising:

appending a digital signature to the string prior to encryption.

3. (Original) The method of Claim 1 further comprising:

inserting the string and a script into a defined portion of the web page to be served.

4. (Previously presented) The method of Claim 3 wherein the defined portion is a locally executed script section of the web page.

5. (Original) The method of Claim 1 further comprising:

serving a script within the web page, the script to decrypt the string and apportion the string to the blank fields.

6. (Original) The method of Claim 1 further comprising:

serving a security applet to the user node; and

receiving login data from the user node encrypted by the security applet.

7. (Original) The method of Claim 6 wherein the login data forms a basis for a key used to encrypt the string.

8. (Previously presented) The method of Claim 6 wherein the security applet is a locally executed applet to perform decryption of the string subsequently sent using a key word from the login data.

9. (Previously presented) The method of Claim 6 further comprising:

comparing the login data to a valid login data to identify if the user is valid; and

denying access if the user node is not valid.

10. (Currently amended) An internet access device having executable instructions that when executed, perform actions ~~A method~~ comprising:

accepting a frame having a resident security applet;

receiving a subframe including a form with a plurality of blank fields;

receiving ~~and~~ an encrypted string;

locally decrypting the encrypted string with the security applet; and

distributing a plurality of portions of the decrypted string to the plurality of blank fields in the form.

11. (Currently amended) The internet access device ~~method~~ of Claim 10 wherein distributing comprises:

parsing the string delimited by embedded length and data type.

12. (Currently amended) The internet access device ~~method~~ of Claim 10 further comprising:

accepting user modification of a field in the form;

encrypting a string using the security applet, the string including at least a content of the field modified; and

transmitting the string to a remote node.

13. (Currently amended) The internet access device ~~method~~ of Claim 10 further comprising:

deriving a key from login data supplied by a user.

14. (Currently amended) The internet access device ~~method~~ of Claim 12 wherein an encryption key is based on login data received from a user.

15. (Currently amended) The internet access device ~~method~~ of Claim 10 further comprising:

generating a login window within the frame;

receiving login data from a user; and

receiving the login data in the security applet.

16. (Previously presented) A computer readable storage media containing executable computer program instructions which when executed cause a digital processing system to perform a method comprising:

concatenating data from a plurality of fields of a requested web page into a string;

encrypting the string;

serving to a user node, the web page and a form corresponding to the requested web page that includes each blank field in the plurality of fields and the encrypted string; and

enabling at least the encrypted string to be locally decrypted at the user node.

17. (Original) The computer readable storage media of Claim 16 which when executed cause a digital processing system to perform a method further comprising:

appending a digital signature to the string prior to encryption.

18. (Original) The computer readable storage media of Claim 16 which when executed cause a digital processing system to perform a method further comprising:

inserting the string and a script into a defined portion of the web page to be served.

19. (Previously presented) The computer readable storage media of Claim 18 which when executed cause a digital processing system to perform a method further comprising:

the defined portion is a locally executed script section of the web page.

20. (Original) The computer readable storage media of Claim 16 which when executed cause a digital processing system to perform a method further comprising:

serving a script within the web page, the script to decrypt the string and apportion the string to the blank fields.

21. (Original) The computer readable storage media of Claim 16 which when executed cause a digital processing system to perform a method further comprising:

serving a security applet to the user node; and

receiving login data from the user node encrypted by the security applet.

22. (Original) The computer readable storage media of Claim 21 the login data forms a basis for a key used to encrypt the string.

23. (Previously presented) The computer readable storage media of Claim 21 wherein the security applet is a locally executed applet to perform decryption of the string subsequently sent using a key word from the login data.

24. (Previously presented) The computer readable storage media of Claim 21 which when executed cause a digital processing system to perform a method further comprising:

comparing the login data to a valid login data to identify if the user is valid; and

denying access if the user node is not valid.

25. – 30. (Canceled)